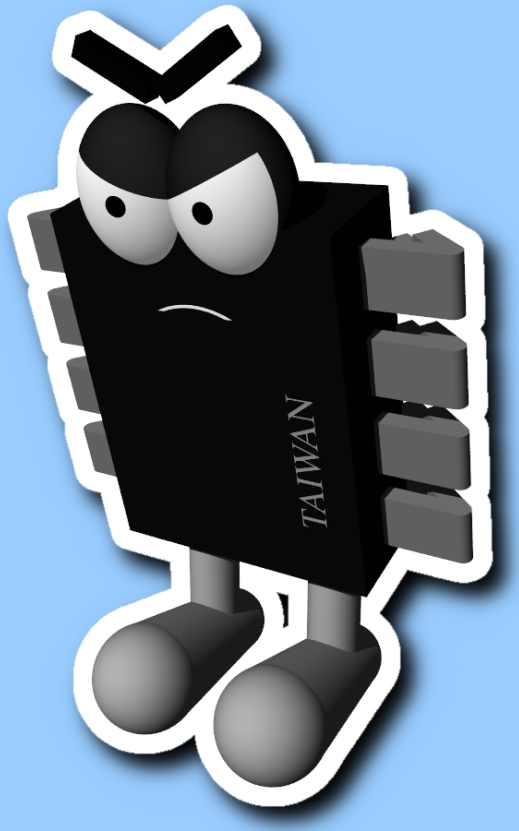
¡Mi aspiradora robot llama a China!



Hackeando mi robot aspirador

Edición corregida y aumentada

Me compré un robot aspirador

- Control desde el móvil (por WiFi)
  - potencia de aspiración
  - modo fregona
  - modo de limpieza
  - control manual
  - activar/desactivar sonido
- Genera mapas
  - más rápido y eficiente que los aleatorios

Primer problema: condiciones de uso

los datos personales que recabamos sobre usted son su **correo electrónico** y la **direccion IP** del dispositivo movil. [...] También recogemos el numero de serie del robot [...] podrá **tener acceso al mapeado** que su robot aspirador registra en su memoria interna [...] En ningun caso [...] geolocaliza el producto. [...] **La empresa desarrolladora de la aplicación movil** es [...], empresa **ubicada en la República Popular de China** [...] Esta empresa [...] se ubica en un tercer país ajeno al Espacio Económico Europeo **cuya legislación en materia de protección de datos no garantiza un nivel de protección adecuado** conforme al reglamento (UE) 2016/679

Segundo problema: permisos de la app

- Hacer fotografías y grabar vídeos
- Leer, modificar o eliminar contenido de la tarjeta SD y la memoria interna
- Grabar audio
- Ubicación precisa (GPS)
- Llamar directamente a números de teléfono
- Acceso completo a Internet
- Ejecutarse al inicio
- Obtener datos del propietario (Retirada en API 9 por ser peligrosa)
- Obtener la lista de procesos (Retirada en API 21 por ser peligrosa)
- Leer los logs del sistema (Not for use by third-party applications, because Log entries can contain the user's private information.)

No puede instalarse en tablets desde Google Play

¿Pero lo hacen realmente?

No necesariamente, pero...

¿Pero lo hacen realmente?

No necesariamente, pero... *queda feo*.

“La mujer del César
no sólo ha de ser buena y virtuosa,
también ha de parecerlo”

Por si fuera poco

- Depende de un servidor exterior
  - Puede fallar Internet
  - Puede fallar el servidor
  - La empresa puede cerrar
  - La empresa puede apagar el servidor

Toca arremangarse

Instalando la app en una tablet

No podemos utilizar Google Play

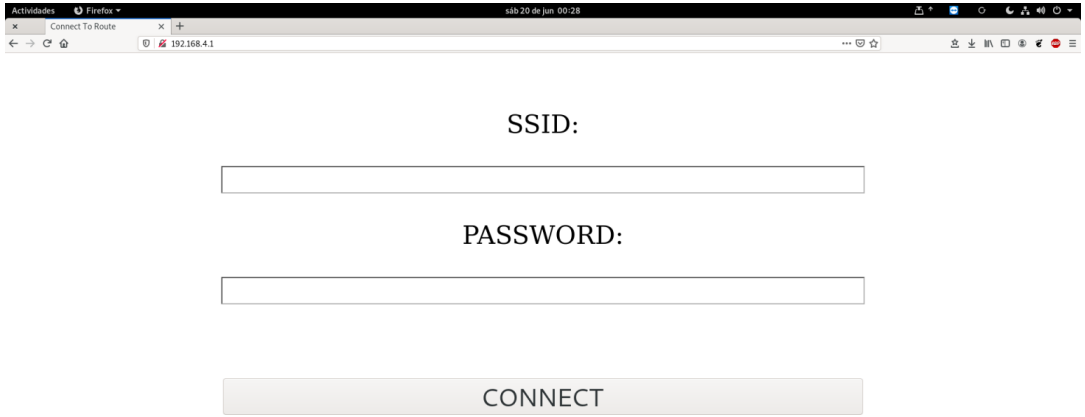
- Borrar la tablet
- Usar correo-e *virgen*
- Descargar el APK
- Desactivar “orígenes de terceros”
- Instalar el APK

Proceso de emparejado WiFi

- La aspiradora se convierte en AP WiFi
  - SSID CongaGyro_XXXXXX
  - IPs 192.168.4.YYY
- Escaneamos los puertos

Escaneamos los puertos y...

Conexión al puerto 80



- No es suficiente
- Solución
  - montar punto de acceso CongaWifi_123456 en RPi
  - lanzar '**nc -l -p 80**'
  - usar la app oficial para emparejar

Resultados de emparejamiento

```
GET /robot/getRobotInfo.do?
ssid=AAAAAAAA&pwd=BBBBBBBB&jDomain=bl-app-
eu.robotbona.com&jPort=8082&sDomain=bl-im-
eu.robotbona.com&sPort=20008&cleanSTime=5 HTTP/1.1
User-Agent: blapp
Accept: application/json
Host: 192.168.4.1
Connection: Keep-Alive
Accept-Encoding: gzip
```

```
HTTP/1.0 200 OK

{
  "result":"0",
  "msg":"OK",
  "version":"1.0",
  "data":{
    "deviceId":"zzzzzzzzzzzzzz",
    "deviceType":"1",
    "appKey":"yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy",
    "authCode":"xxxxxx",
    "errorCode":"0xnnnnnnnn"
  }
}
```

Escaneo de puertos en la aspiradora...

Resultados de emparejamiento (2)

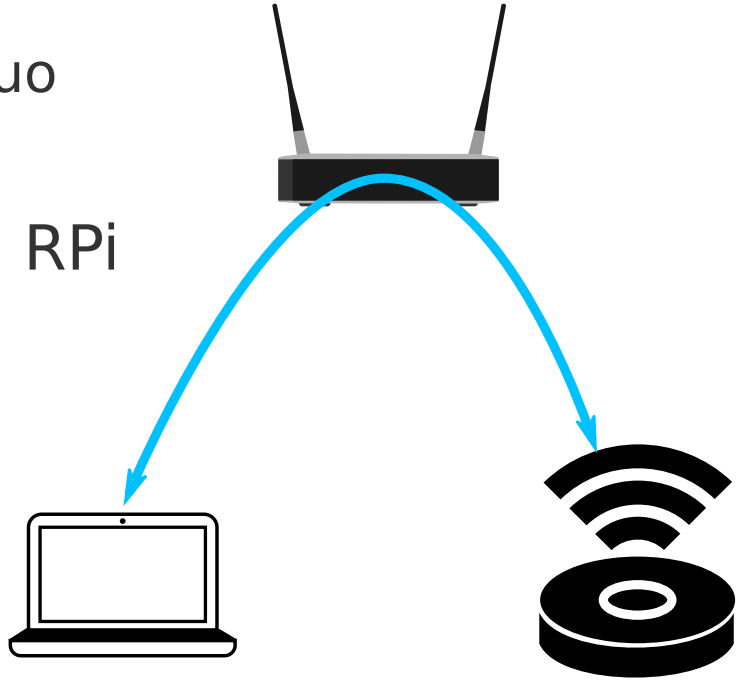
¡¡¡El puerto 8888 está abierto!!!

Analizando las comunicaciones

- Es difícil *esnifar* una WiFi
  - adaptador que acepte modo promiscuo
  - configuración liosa

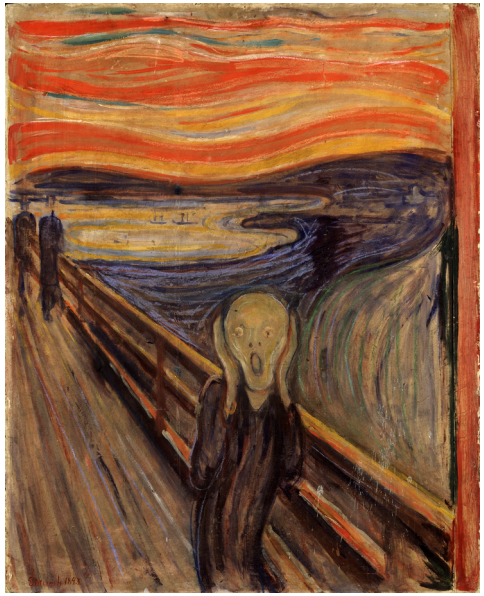
Analizando las comunicaciones

- Es difícil *esnifar* una WiFi
  - adaptador que acepte modo promiscuo
  - configuración liosa
- Más sencillo: montar un AP con una RPi
  - Todo el tráfico para por el AP siempre
  - Permite aislar el robot de Internet
  - Captura con **TCPDUMP**
  - Análisis con Wireshark



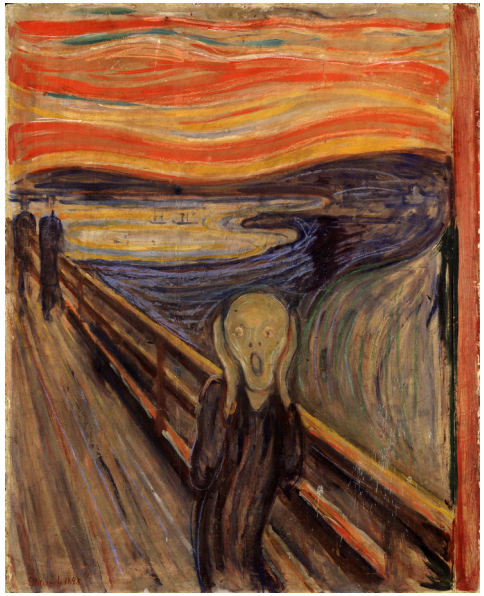
Analizando las comunicaciones

Tras emparejar con el nuevo AP... ¡el puerto 8888 ha desaparecido!



Analizando las comunicaciones

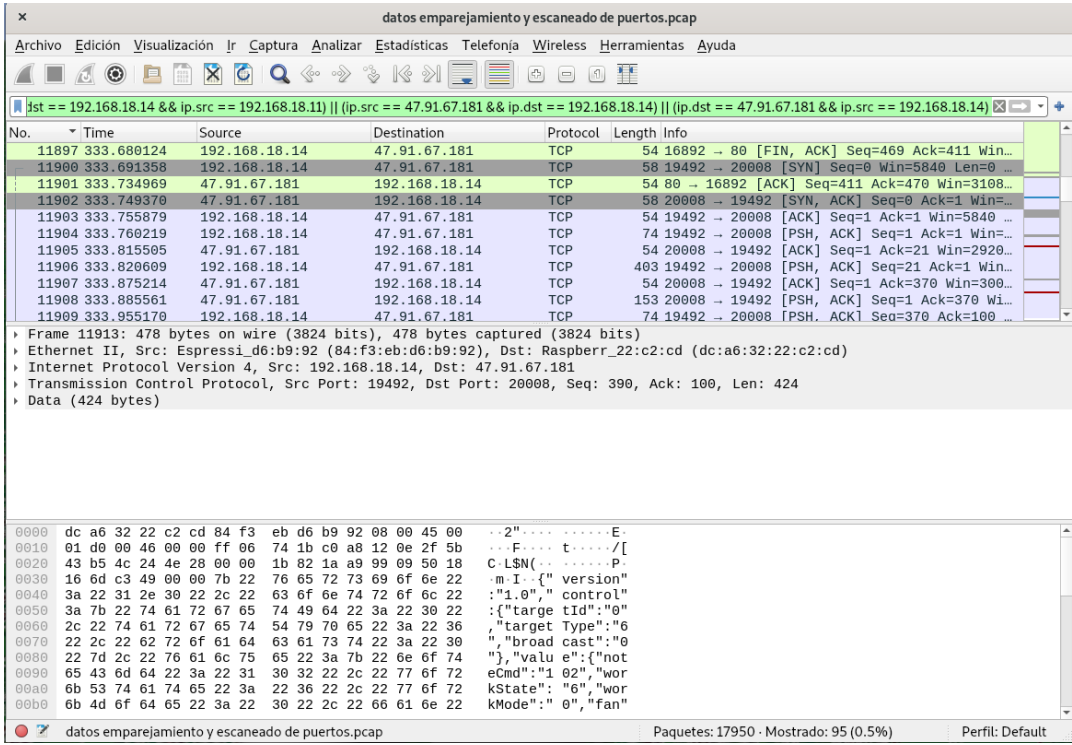
Tras emparejar con el nuevo AP... ¡el puerto 8888 ha desaparecido!



Ya lo investigaremos más tarde...

Entrando en harina

- Activamos NAT en AP
- Iniciamos TCPDUMP en AP
- Encendemos el robot y la tablet
- Lanzamos comandos
  - limpiar
  - parar
  - volver a la base
  - modo de limpieza...
- Paramos TCPDUMP
- Abrimos Wireshark



Analizando las comunicaciones

- dos conexiones HTTP desde el robot a **bl-app-eu.robotbona.com**
- una conexión (permanente) desde el robot al puerto 20008 de **bl-im-eu.robotbona.com**
- conexión cifrada entre tablet y servidor
  - pasamos de ella

Analizando las comunicaciones

- dos conexiones HTTP desde el robot a **bl-app-eu.robotbona.com**
- una conexión (permanente) desde el robot al puerto 20008 de **bl-im-eu.robotbona.com**
- conexión cifrada entre tablet y servidor
  - pasamos de ella
- ¡No hay comunicación entre la tablet y el robot!

Analizando las comunicaciones

- **Primera conexión HTTP**
  - formato URLEncoded

```
appKey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
deviceId=yyyyyyyyyyyyyy
deviceType=1
clearTime=0
```

- **Respuesta**
  - formato Chunked

```
2b
{"msg":"ok","result":"0","version":"1.0.0"}
0
```

Analizando las comunicaciones

- **Segunda conexión HTTP**
  - formato URLEncoded

```
appKey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
authCode=zzzzz
deviceId=yyyyyyyyyyyyy
deviceType=1
funDefine=11101
nonce_str=AAAAA
version={"wifi":"1.0.48","mcu":"3.9.1714(513)"}
sign=SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS
```

- **Respuesta**
  - formato Chunked

```
2b
{"msg":"ok","result":"0","version":"1.0.0"}
0
```

Analizando las comunicaciones

- **Segunda conexión HTTP**
  - formato URLEncoded

```
appKey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
authCode=zzzzz
deviceId=yyyyyyyyyyyyy
deviceType=1
funDefine=11101
nonce_str=AAAAA
version={"wifi":"1.0.48","mcu":"3.9.1714(513)"}
sign=SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS
```

- **Respuesta**
  - formato Chunked

```
2b
{"msg":"ok","result":"0","version":"1.0.0"}
0
```

- Tras esto, sigue en el puerto 20008

Suplantando al servidor HTTP

- Construimos un miniservidor HTTP en python
- netcat en puerto 20008
- Suplanta al servidor oficial -> mismas respuestas
- Modificamos nuestro DNS

Suplantando al servidor HTTP

- Construimos un miniservidor HTTP en python
- netcat en puerto 20008
- Suplanta al servidor oficial -> mismas respuestas
- Modificamos nuestro DNS
- ¡¡¡NO FUNCIONA!!!

Suplantando al servidor HTTP

- Construimos un miniservidor HTTP en python
- netcat en puerto 20008
- Suplanta al servidor oficial -> mismas respuestas
- Modificamos nuestro DNS
- ¡¡¡NO FUNCIONA!!!
- Cambiamos campos y formatos para hacerlos idénticos byte a byte

Suplantando al servidor HTTP

- Construimos un miniservidor HTTP en python
- netcat en puerto 20008
- Suplanta al servidor oficial -> mismas respuestas
- Modificamos nuestro DNS
- ¡¡¡NO FUNCIONA!!!
- Cambiamos campos y formatos para hacerlos idénticos byte a byte
- ¡¡¡SIGUE SIN FUNCIONAR!!!

Por qué falla

- Espera los datos en un único paquete IP

```
HTTP/1.1 200 \r\n
Date: Sat, 27 Jun 2020 16:38:08 GMT\r\n
Content-Type: application/json;charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: close\r\n
Set-Cookie: SERVERID=abcdefghijklmnopqrstuvwxyz12345|1234567890|12345678
\r\n
2b\r\n
{"msg":"ok","result":"0","version":"1.0.0"}\r\n
```

```
0\r\n
\r\n
```

Por qué falla (2)

- Yo los enviaba en dos paquetes separados

```
HTTP/1.1 200 \r\n
Date: Sat, 27 Jun 2020 16:38:08 GMT\r\n
Content-Type: application/json;charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: close\r\n
Set-Cookie: SERVERID=abcdefghijklmnopqrstuvwxyz12345|1234567890|12345
\r\n
```

```
2b\r\n
{"msg":"ok","result":"0","version":"1.0.0"}\r\n
0\r\n
\r\n
```

Por qué falla (3)

- En TCP debería dar igual hacerlo de cualquiera de las dos maneras
- ¿Protección contra hackeos? ¿Chapuza?

Por qué falla (3)

- En TCP debería dar igual hacerlo de cualquiera de las dos maneras
- ¿Protección contra hackeos? ¿Chapuza?

Analizando las comunicaciones

- Datos en puerto 20008
  - 369 bytes: 20 bytes + JSON

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
  "version":"1.0",
  "control":{
    "targetId":"0",
    "targetType":"6",
    "broadcast":"0"
  },
  "value":{
    "token":"bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb",
    "deviceId":"yyyyyyyyyyyyyy",
    "appKey":"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "deviceType":"1",
    "authCode":"zzzzz",
    "deviceIp":"192.168.18.3",
    "devicePort":"8888",
    "firmwareVer":"{\"wifi\":\"1.0.48\",\"mcu\":\"3.9.1714(513)\"}"
  }
}
```

Respuesta Servidor: 99 bytes, mismo formato

```
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
   "msg":"login succeed",
   "result":0,
   "version":"1.0",
   "time":"2020-06-21-04-59-39"
}
```

Analizando las comunicaciones

- Datos en puerto 20008
  - 369 bytes: 20 bytes + JSON

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
  "version":"1.0",
  "control":{
    "targetId":"0",
    "targetType":"6",
    "broadcast":"0"
  },
  "value":{
    "token":"bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb",
    "deviceId":"yyyyyyyyyyyyyy",
    "appKey":"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
    "deviceType":"1",
    "authCode":"zzzzz",
    "deviceIp":"192.168.18.3",
    "devicePort":"8888",
    "firmwareVer":"{\"wifi\":\"1.0.48\",\"mcu\":\"3.9.1714(513)\"}"
  }
}
```

Respuesta Servidor: 99 bytes, mismo formato

```
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
   "msg":"login succeed",
   "result":0,
   "version":"1.0",
   "time":"2020-06-21-04-59-39"
}
```

¡¡¡¡El puerto 8888 vuelve a estar abierto!!!!

Siguiente paquete

Envío: 444 bytes

```
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 03 00 00 00 | 00 00 00 00
{
  "version":"1.0",
  "control": {
    "targetId":"0",
    "targetType":"6",
    "broadcast":"0"
  },
  "value": {
    "noteCmd":"102",
    "workState":"6",
    "workMode":"0",
    "fan":"1",
    "direction":"0",
    "brush":"2",
    "battery":"100",
    "voice":"2",
    "error":"0",
    "standbyMode":"1",
    "waterTank":"40",
    "clearComponent":"0",
    "waterMark":"0",
    "version":"3.9.1714(513)",
    "attract":"0",
    "deviceIp":"192.168.18.14",
    "devicePort":"8888",
    "cleanGoon":"2",
    "extParam":"{\"cleanModule\":\"3\"}"
  }
}
```

Respuesta: 60 bytes

```
3c 00 00 00 | 19 00 c8 00 | 01 00 00 00 | 03 00 00 00 | 01 00 00 00
{
  "msg":"OK",
  "result":0,
  "version":"1.0"
}\n
```

Siguientes paquetes

Envío: 20 bytes (sin JSON)
Respuesta: 20 bytes (sin JSON)
Intervalo de envío: 30 segundos por cada par -> PING

```
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 04 00 00 00 | e7 03 00 00

14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 04 00 00 00 | e7 03 00 00

14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 05 00 00 00 | e7 03 00 00

14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 05 00 00 00 | e7 03 00 00

14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 06 00 00 00 | e7 03 00 00

14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 06 00 00 00 | e7 03 00 00
```

Aparece un patrón

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 03 00 00 00 | 00 00 00 00
{
3c 00 00 00 | 19 00 c8 00 | 01 00 00 00 | 03 00 00 00 | 01 00 00 00
{
  "msg": "OK"
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 06 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 06 00 00 00 | e7 03 00 00
```

Aparece un patrón

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 03 00 00 00 | 00 00 00 00
{
3c 00 00 00 | 19 00 c8 00 | 01 00 00 00 | 03 00 00 00 | 01 00 00 00
{
  "msg": "OK",

14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 04 00 00 00 | e7 03 00 00

14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 04 00 00 00 | e7 03 00 00

14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 05 00 00 00 | e7 03 00 00

14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 05 00 00 00 | e7 03 00 00

14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 06 00 00 00 | e7 03 00 00

14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 06 00 00 00 | e7 03 00 00
```

Número de secuencia

Aparece un patrón

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 03 00 00 00 | 00 00 00 00
{
3c 00 00 00 | 19 00 c8 00 | 01 00 00 00 | 03 00 00 00 | 01 00 00 00
{
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 06 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 06 00 00 00 | e7 03 00 00
```

Número de secuencia

No es CRC
¿Tipo de paquete?

Aparece un patrón

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 03 00 00 00 | 00 00 00 00
{
3c 00 00 00 | 19 00 c8 00 | 01 00 00 00 | 03 00 00 00 | 01 00 00 00
{
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 06 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 06 00 00 00 | e7 03 00 00
```

Tamaño de la trama

Número de secuencia

No es CRC
¿Tipo de paquete?

Aparece un patrón

```
71 01 00 00 | 10 00 00 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
63 00 00 00 | 11 00 c8 00 | 01 00 00 00 | 02 00 00 00 | 00 00 00 00
{
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 03 00 00 00 | 00 00 00 00
{
3c 00 00 00 | 19 00 c8 00 | 01 00 00 00 | 03 00 00 00 | 01 00 00 00
{
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 04 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 05 00 00 00 | e7 03 00 00
14 00 00 00 | 00 01 c8 00 | 01 00 00 00 | 06 00 00 00 | e7 03 00 00
14 00 00 00 | 11 01 c8 00 | 01 00 08 01 | 06 00 00 00 | e7 03 00 00
```

Tamaño de la trama

Número de secuencia

Indica origen y pregunta/respuesta
¿Tipo de paquete?
No es CRC

No es CRC
¿Tipo de paquete?

Buscando comandos

- Programa específico para separar tramas
- Buscamos los comandos:

```
d1 00 00 00 | fa 00 c8 00 | 00 00 09 01 | 1a 27 00 00 | 00 00 00 00
{
  "cmd":0,
  "control":{
    "authCode":"240727",
    "deviceIp":"192.168.18.3",
    "devicePort":"8888",
    "targetId":"zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz",
    "targetType":"3"
  },
  "seq":0,
  "value":{"transitCmd":"ID_COMANDO"}
}\n
```

Comandos encontrados

- 98: actualizar estado
- 100: limpiar
- 102: parar
- 104: volver a base
- 106: modo de limpieza
- 108: control manual
- 110: potencia de aspirado
- 123: activar pitidos
- 125 desactivar pitidos
- 131: actualizar mapa
- 143: encontrar al robot
- 145: modo de fregado
- 400: lista de programas
- 402: añadir programa
- 404: borrar programa

Comandos encontrados

- 98: actualizar estado
- 100: limpiar
- 102: parar
- 104: volver a base
- 106: modo de limpieza
- 108: control manual
- 110: potencia de aspirado
- 123: activar pitidos
- 125 desactivar pitidos
- 131: actualizar mapa
- 143: encontrar al robot
- 145: modo de fregado
- 400: lista de programas
- 402: añadir programa
- 404: borrar programa
- 139: actualizar la hora
- 127: actualizar el firmware

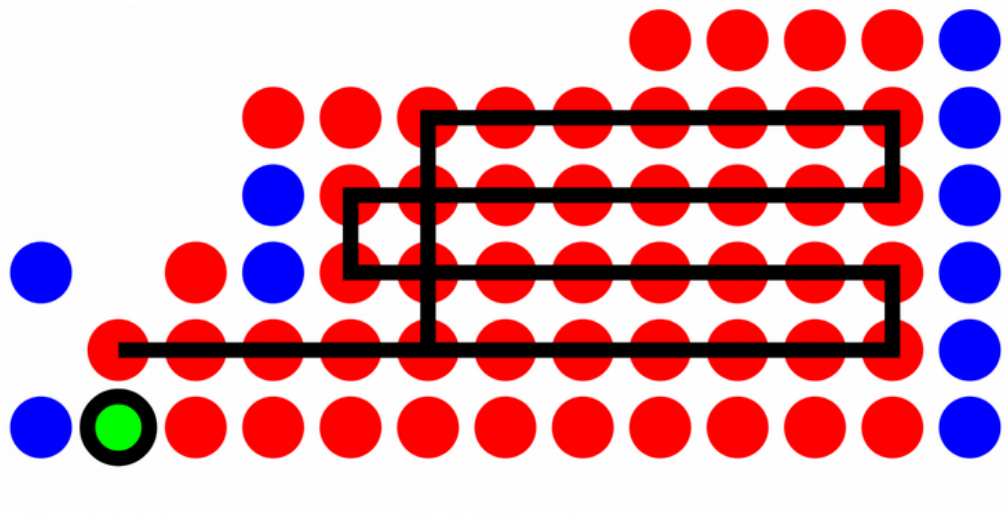
Estado del robot

```
bc 01 00 00 | 18 00 00 00 | 01 00 00 00 | 1a 00 00 00 | 00 00 00 00
{
  "version":"1.0",
  "control":{
    "targetId":"0",
    "targetType":"6",
    "broadcast":"0"
  },"value":{
    "noteCmd":"102",
    "workState":"5",
    "workMode":"0",
    "fan":"2",
    "direction":"0",
    "brush":"2",
    "battery":"100",
    "voice":"1",
    "error":"0",
    "standbyMode":"1",
    "waterTank":"40",
    "clearComponent":"0",
    "waterMark":"0",
    "version":"3.11.416(513)",
    "attract":"0",
    "deviceIp":"192.168.18.3",
    "devicePort":"8888",
    "cleanGoon":"2",
    "extParam":"{\"cleanModule\":\"3\"}"
  }
}
```

Mapas


```
{
  "version": "1.0",
  "control": {
    "targetId": "0",
    "targetType": "6",
    "broadcast": "0"
  },
  "value": {
    "noteCmd": "101",
    "clearArea": "0",
    "clearTime": "10",
    "clearSign": "2020-06-24-01-31-41-2",
    "clearModule": "11",
    "isFinish": "1",
    "chargerPos": "8,12",
    "map": "AAAAAAAAZABk0vwAaoDXAGpA1wBqgNcAqNL8AA==",
    "track": "AQAEADIxMzExMTEy"
  }
}
```


- Codificación RLE
- Zonas recorridas
- Posición de la base



Control manual

- Se conecta al puerto 8888 (¡por fin!)
- Protocolo parecido... pero no idéntico

```
d1 00 00 00 | fa 00 c8 00 | 00 00 29 27 | 28 27 00 00 | 00 00 00 00
d1 00 00 00 | fa 00 c8 00 | 00 00 2c 27 | 2b 27 00 00 | 00 00 00 00
d1 00 00 00 | fa 00 c8 00 | 00 00 2f 27 | 2e 27 00 00 | 00 00 00 00
d1 00 00 00 | fa 00 c8 00 | 00 00 32 27 | 31 27 00 00 | 00 00 00 00
db 00 00 00 | fa 00 c8 00 | 00 00 35 27 | 34 27 00 00 | 00 00 00 00
```

Control manual (2)

- Problemas
  - ¿qué pasa con números mayores de 0xFFFF?
  - Es un rollo abrir un nuevo socket

```
d1 00 00 00 | fa 00 c8 00 | 00 00 29 27 | 28 27 00 00 | 00 00 00 00
d1 00 00 00 | fa 00 c8 00 | 00 00 2c 27 | 2b 27 00 00 | 00 00 00 00
d1 00 00 00 | fa 00 c8 00 | 00 00 2f 27 | 2e 27 00 00 | 00 00 00 00
d1 00 00 00 | fa 00 c8 00 | 00 00 32 27 | 31 27 00 00 | 00 00 00 00
db 00 00 00 | fa 00 c8 00 | 00 00 35 27 | 34 27 00 00 | 00 00 00 00
```

Control manual (3)

- ¿Es posible controlarla desde el servidor?
  - raro: no vamos a controlarla desde el bar
  - legítimo: podemos tener varias WiFis en casa
    - móvil conectado a una, robot a otra

Control manual (3)

- ¿Es posible controlarla desde el servidor?
  - raro: no vamos a controlarla desde el bar
  - legítimo: podemos tener varias WiFis en casa
    - móvil conectado a una, robot a otra

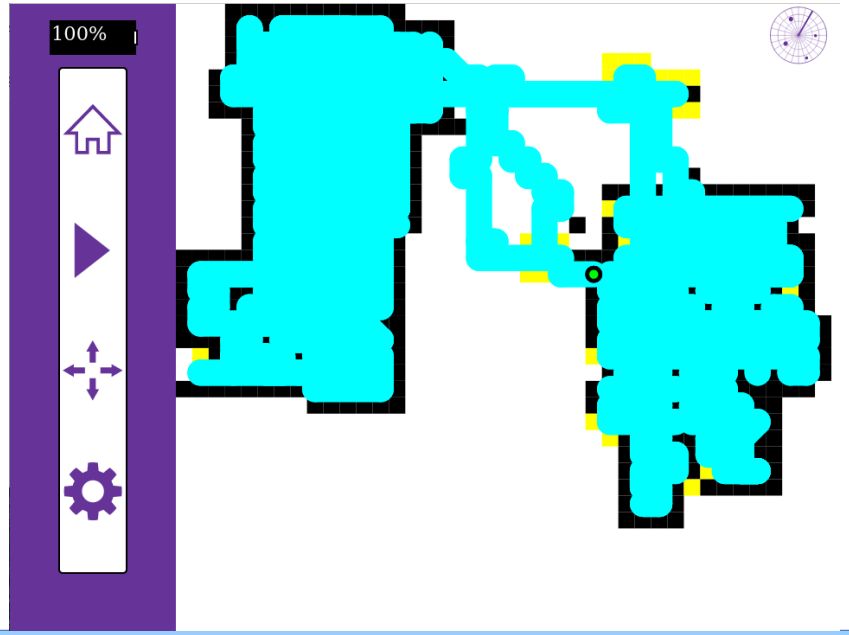
¡¡¡¡¡¡¡Se puede!!!!!!!

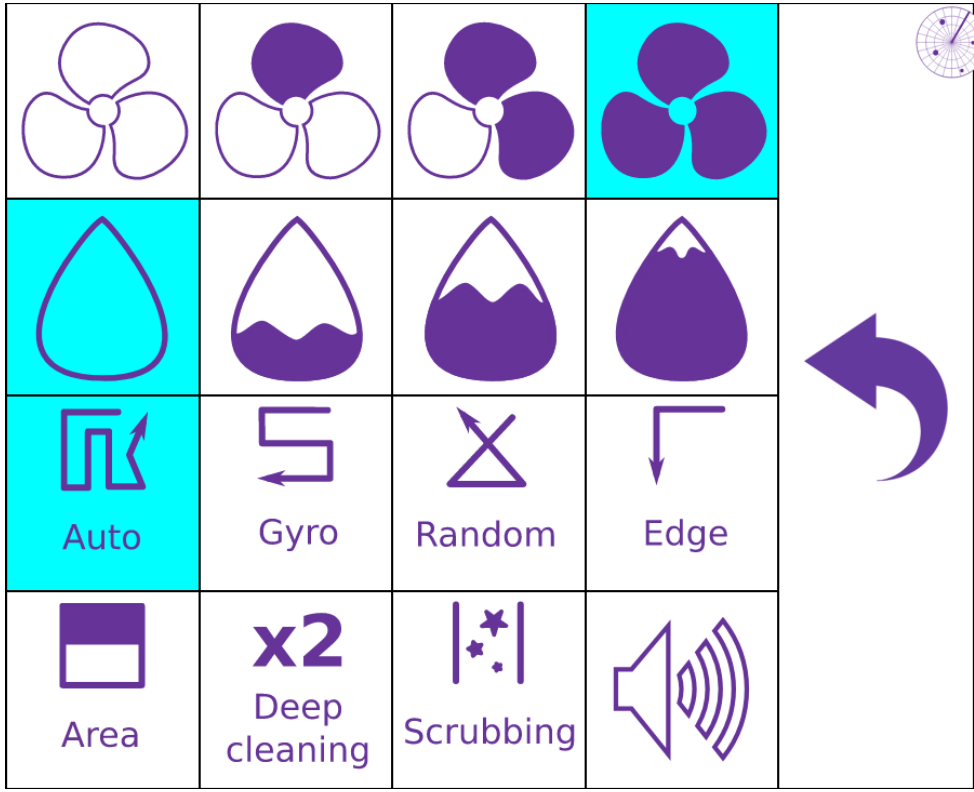
Control manual (4)

- Comando 108, más parámetro de dirección
  - tiene que enviarse repetidamente cada dos segundos
  - dirección 1 -> avanzar
  - dirección 2 -> retroceder
  - dirección 3 -> girar a la izquierda
  - dirección 4 -> girar a la derecha
  - dirección 5 -> detenerse

La nueva APP

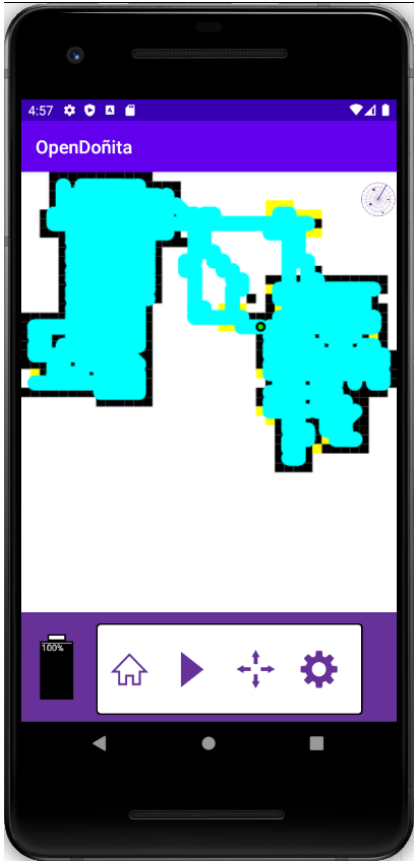
- Hecha en python
- Control por web (javascript)





App para Android

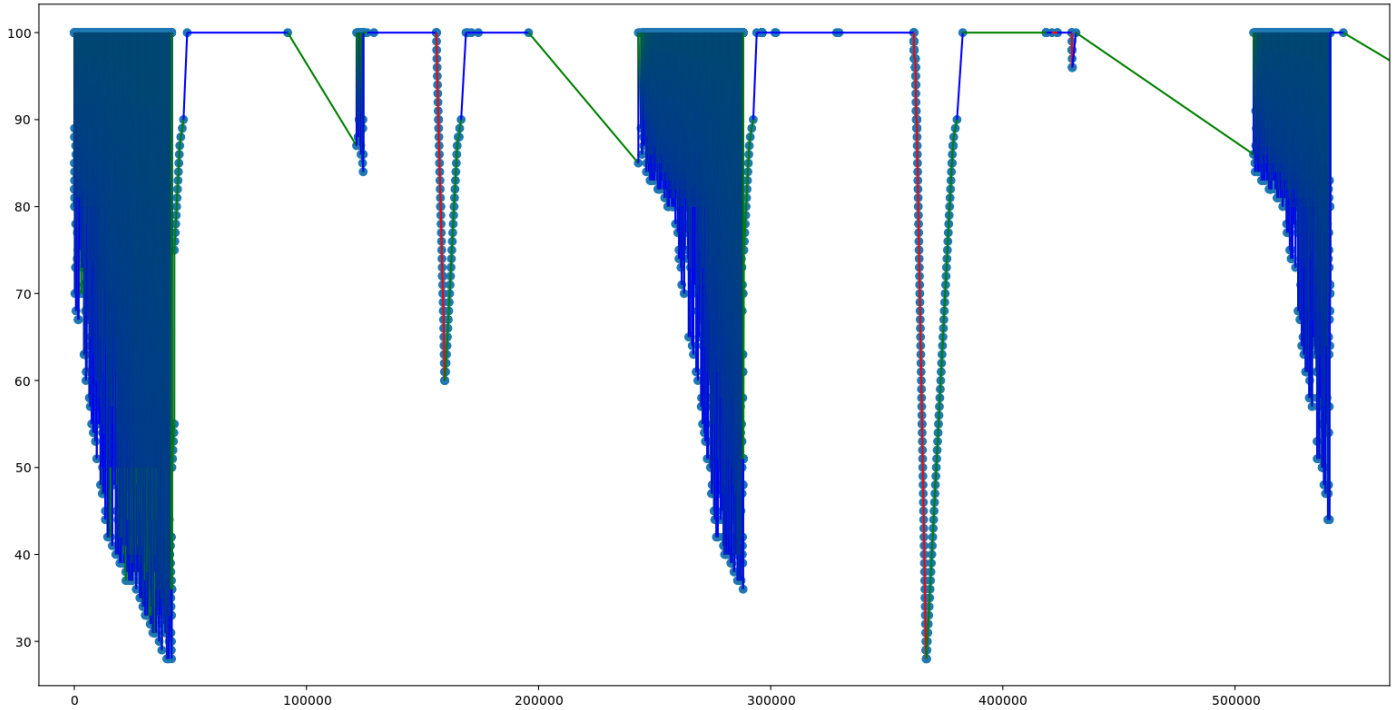
- Basada en WebView
- Utiliza uPnP para encontrar el servidor
  - módulo iot-upnp de python en servidor
  - código *a pelo* en la app
  - se basa sólo en el UUID



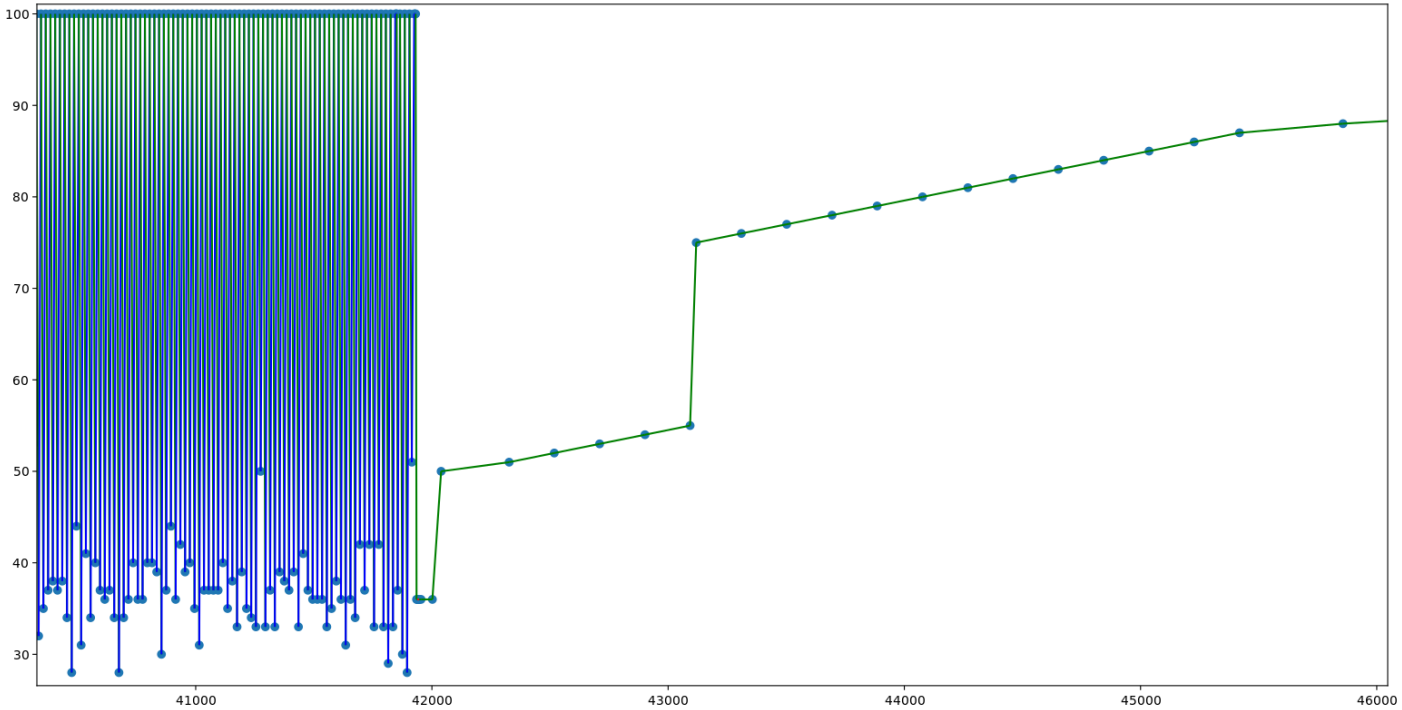
Problema de carga de la batería

- Comportamiento extraño del robot si lleva mucho tiempo en la base
  - se queda sin batería al poco de empezar a aspirar
  - cambia de “cargando” a “cargado” y viceversa cada quince segundos
  - nivel de batería baja progresivamente en lugar de cargar

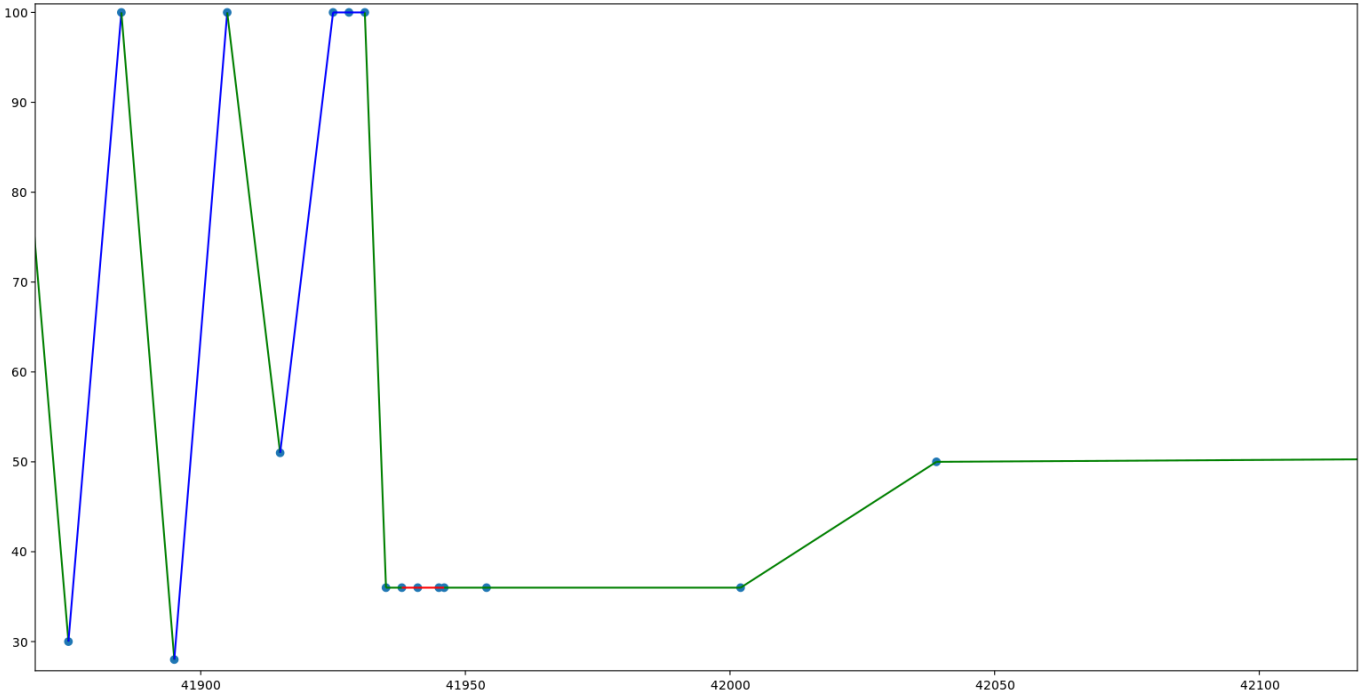
Problema de carga de la batería



Problema de carga de la batería



Problema de carga de la batería



Problema de carga de la batería

- Cuando lleva mucho rato en la base, la batería empieza a descargarse
- Conmuta de estado cada quince segundos (aprox)
  - “cargado”, 100% batería
  - “cargando”, <85% batería (y bajando)

Problema de carga de la batería

- Cuando lleva mucho rato en la base, la batería empieza a descargarse
- Conmuta de estado cada quince segundos (aprox)
  - “cargado”, 100% batería
  - “cargando”, <85% batería (y bajando)
- Solución: quitarla de la base y volverla a poner
  - vuelve a cargar la batería y aguanta de nuevo un día (aprox)

Problema de carga de la batería

- Cuando lleva mucho rato en la base, la batería empieza a descargarse
- Conmuta de estado cada quince segundos (aprox.)
  - “cargado”, 100% batería
  - “cargando”, <85% batería (y bajando)
- Solución: quitarla de la base y volverla a poner
  - vuelve a cargar la batería y aguanta de nuevo un día (aprox.)

¡¡¡¡¡SE PUEDE AUTOMATIZAR!!!!!

Actualización del firmware

- Obliga a utilizar la app original
- Implica conectar el robot a Internet

Actualización del firmware

- Obliga a utilizar la app original
- Implica conectar el robot a Internet
  - roooollooooo

Actualización del firmware

- Obliga a utilizar la app original
- Implica conectar el robot a Internet
  - roooollooooo
- Alternativa: crear un emulador de robot
  - Se conectaría al servidor del fabricante
  - Simularía ser mi robot
  - Nunca enviaría datos privados

Emulador de robot

Riesgo de problemas legales

Emulador de robot

- Como mínimo, zona gris
  - Nos estamos conectando a un servidor que no es nuestro
  - Protocolo no estándar (=desconocido)
    - ¿Qué hacer ante un paquete desconocido?
  - No sabemos la calidad de su programación
    - ¿Y si metemos la pata y se cuelga?
    - Riesgo de dejar al resto de usuarios sin servicio

Emulador de robot

¡¡¡¡Descartado!!!!

Gracias por vuestra atención